ABSTRACT

METHOD AND SYSTEM FOR SECURING SCRAMBLED DATA

The invention relates to a distribution process with access control of scrambled data to at least one receiver terminal.

The process according to the present invention comprises :

a first encryption phase comprising the following stages:

- subdividing said data into an integer of families Fj (j = 1...M) each comprising an integer of blocks Bi (i = 1...N),

- assigning each family Fj a specific identification parameter pj (j = 1...M) associated with at least one descrambling module Mj having a specific processing capacity and a level of security,

- scrambling each block Bi of a family Fj of type pj by a key Kj (j = 1...M) in biunivocal relation with the parameter pj,

and a second descrambling phase comprising the following stages:

- identifying the family of each block Bi,

- descrambling each block Bi of a family of type pj by the module Mj by means of the key Kj.

(Figure 4)